



State of West Virginia Office of Technology

Policy: **Information Security**

Issued by the CTO

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 1 of 20

1.0 PURPOSE (Underlined terms are defined in Section 7.0 of document)

This policy, issued by the [West Virginia Office of Technology](#) (OT), establishes objectives and responsibilities for all West Virginia state government agencies, [employees](#), vendors, and business associates, specifically the Executive, regarding [Information Security](#) and the protection of [information resources](#).

2.0 SCOPE

This document applies to all employees with access to information and the systems that store, access, or process that information.

The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided [Information Technology](#) (IT) resources and is not necessarily all-inclusive. IT resources may include anything with a processor, communications capability, or data storage. (See Appendix A, "Technology Usage Practices" for a list of examples.)

Questions about specific security-related uses which are not detailed in this policy should be directed to a supervisor or manager.

3.0 BACKGROUND

Under the provisions of West Virginia Code 5A-6-4a, the [Chief Technology Officer \(CTO\)](#) is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent. The Governor's Executive Order No. 6-06, signed on August 16, 2006, empowers the CTO to "issue information security policies applicable to all Executive Branch department-level organizations."

Policy: [Information Security](#)

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 2 of 20

This policy is one in a series of IT related policies intended to define and enable the incorporation of appropriate practices into all activities using technology in the State of West Virginia.

4.0 RELEVANT DOCUMENTS/MATERIAL

- 4.1 [West Virginia Office of Technology \(OT\) Web Site Home Page](#)
 - 4.2 [OT - IT Security Web Page](#)
 - 4.3 [OT Policies Issued by the Chief Technology Officer \(CTO\)](#)
 - 4.4 [West Virginia Code §5A-6-4a](#) – “Duties of the Chief Technology Officer Relating to Security of Government Information”
-

5.0 RESPONSIBILITY/REQUIREMENTS

5.1 Administration

- 5.1.1 The authorized head of each agency (agency head) must assign the role of [Information Security Administrator](#) (ISA). The ISA must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy.
 - 5.1.1.1 If necessary, the ISA may delegate duties to one or more individuals {ex: [Information Security Liaisons](#) (ISL)} whose main function will be to assist in the protection of information resources within their agency.
- 5.1.2 All IT assets, including hardware, software, and data, are owned by the State, unless excepted by contractual agreement.
 - 5.1.2.1 [Users](#) are required to comply with legal protection granted to programs and data by copyright and license.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 3 of 20

No unauthorized software will be installed on State systems.

5.1.2.1.1 The OT or its equivalent will authorize all software installation.

5.1.3 Users will utilize, maintain, disclose, and dispose of all information resources, regardless of [medium](#), according to law, regulation, and/or policy.

5.1.4 The ISA will ensure that a risk management program will be implemented and documented, and that a [risk analysis](#) will be conducted periodically.

5.1.5 The ISA will oversee and ensure that cost effective contingency response and recovery plans will be maintained, providing for prompt and effective restoration of critical data systems and business functions in the event of any disruptive incident.

5.1.5.1 [Procedures](#), guidelines, and mechanisms utilized during an Information [Security incident](#), along with the roles and responsibilities of the incident management teams, must be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.

5.1.5.2 Testing will be performed at intervals designated within CTO standards.

5.2 [Access Controls](#)

5.2.1 Access controls must be consistent with all state and federal laws and statutes, and will be implemented in accordance with this policy.

5.2.2 The OT, working with designated individuals, will develop procedures to protect information resources from accidental,

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 4 of 20

unauthorized, or malicious access, disclosure, modification, or destruction.

5.2.3 Appropriate controls must be established and maintained to protect the confidentiality of [passwords](#) used for [authentication](#).

5.2.3.1 Passwords are [confidential](#) and must **not** be shared with anyone under any circumstances.

5.2.3.2 Passwords must conform to established standards, and will be changed at intervals designated by the CTO.

5.2.4 All access to computing resources will be granted on a need-to-use basis.

5.2.5 Individual users must be assigned unique [userids](#).

5.2.6 Each employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.

5.2.7 When an employee is terminated, all access will be disabled immediately, unless otherwise approved in writing by appropriate management.

5.2.8 When an employee transfers, all access will be modified to accommodate new roles and responsibilities.

5.3 Data/Information Assets

5.3.1 Confidential, private, [personally identifiable information](#) (PII) or sensitive data (i.e. credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 5 of 20

5.3.2 All [information assets](#) must be accounted for and have an assigned [owner](#).

5.3.2.1 Owners, [custodians](#), and users of information resources must be identified and their responsibilities defined and documented.

5.3.3 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information, according to a classification scheme common to all State agencies.

5.3.3.1 Classification should consider legal protections, privacy, sensitivity, and criticality to the functions of the business.

5.3.4 The owner or custodian will determine and document, and the agency ISA will ensure, the protective guidelines that apply for each level of information. They include, but may not be limited to the following:

- Access
- Use Within <Agency>
- Disclosure Outside <Agency>
- Electronic Distribution
- Disposal/Destruction

5.3.4.1 If, at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

5.4 Personnel Practices

5.4.1 Information resources are designated for authorized purposes. Only minimal personal use of State-provided IT resources is allowed, and should not interfere with the legitimate business of the State.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 6 of 20

- 5.4.1.1 Employees should have no expectation of privacy while using State-provided information resources.
- 5.4.1.2 The State reserves the right to filter Internet site availability, and monitor and review employee use as required for legal, audit, or legitimate authorized State operational or management purposes.
- 5.4.2 The agency head must assure that all employees receive an appropriate background check (where applicable) consistent with legislative rule and [West Virginia Division of Personnel](#) policy.
- 5.4.3 The agency head must assure that all employees sign a confidentiality agreement upon hire and annually thereafter. This confirms that the employee has read, fully comprehends, and will abide by State policies and procedures regarding privacy and information security.
- 5.4.4 The agency head must assure that all employees and others who [access](#) computer systems, will receive sufficient training in policies and procedures, security requirements, correct use of information resources, and other administrative controls.
- 5.4.5 All employees must adhere to rules regarding acceptable and unacceptable uses of IT resources. (See Appendix A “Technology Usage Practices”)
 - 5.4.5.1 Employees must not intentionally introduce a virus into a State-provided computer, or withhold information necessary for effective virus control procedures.
 - 5.4.5.2 Employees must NEVER execute programs or open e-mail attachments that: (1) have not been requested; or (2) come from an unknown source.
 - 5.4.5.2.1 If in doubt and lacking assurance from the sender, employees should contact the OT Service Desk for assistance.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 7 of 20

5.4.5.3 Employees must never attempt to disable, defeat, or circumvent any security firewalls, proxies, screening programs, or other security controls.

5.4.6 Users should report any notice of attempted security or privacy violations to a designated [security contact](#), the agency [Privacy Officer](#), or an immediate supervisor.

5.4.7 Users should immediately report all Information Security incidents to the CTO, the [Chief Information Security Officer](#) (CISO), or the OT Service Desk. Users must provide the following information, to the extent possible:

5.4.7.1 Point of contact (name, phone, e-mail);

5.4.7.2 Characteristics of incident;

5.4.7.3 Date and time incident was detected;

5.4.7.4 Extent of impact;

5.4.7.5 Nature of incident, if known (ex: unauthorized access, system breach or malfunction, data loss or exposure, defacement, other); and

5.4.7.6 Any actions taken in response to the incident.

5.5 Physical and Environmental Security

5.5.1 Information resource facilities will be physically secured by measures appropriate to their critical importance.

5.5.2 Security vulnerabilities will be determined, and controls will be established, to detect and respond to [threats](#) to facilities and physical resources.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 8 of 20

5.5.3 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

5.5.4 Equipment will be secured and protected from physical and environmental damage.

5.5.5 Equipment used outside State premises will be given an equal or greater degree of security protection as that of on-site information resource equipment.

6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based on recommendations of the OT and the [West Virginia Division of Personnel](#).

7.0 DEFINITIONS

7.1 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

7.2 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

7.3 Authentication – The process of verifying the identity of a user.

7.4 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

7.5 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 9 of 20

- 7.6 Confidential Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.
- 7.7 Contractor – Anyone who has a contract with the State or one of its entities.
- 7.8 Custodian of Information – The person or unit assigned to supply services associated with the data.
- 7.9 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security, the term “employee” shall include the following: contractors, subcontractors, contractors’ employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the OT to be subject to this policy. This definition does not create any additional rights or duties.
- 7.10 Information Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
- 7.11 Information Resources – All information assets, in all known formats.
- 7.12 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.
- 7.13 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency’s compliance with State Information Security policies and procedures. The ISA is the agency’s internal and external point of contact for all Information Security matters.
- 7.14 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of [information resources](#).

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 10 of 20

- 7.15 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.
- 7.16 Medium – Any repository, including paper, used to record, maintain, or install information or data.
- 7.17 Owner of Information – The person(s) ultimately responsible for an application and its data viability.
- 7.18 Password – A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.
- 7.19 Personally Identifiable Information (PII) – Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.
- 7.20 Privacy Officer - The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.
- 7.21 Procedure – A set of instructions or process steps prescribed in sufficient detail in order to understand how to meet a policy requirement. Procedures should document roles, methods, options, and examples necessary for a reader to understand how to comply with a policy.
- 7.22 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.
- 7.23 Security Contact – These individuals include the ISA or the ISL.
- 7.24 Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/07

Revision Date:

Page 11 of 20

- 7.25 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of Information Security.
- 7.26 User – A person authorized to access an information resource.
- 7.27 Userid – A unique “name” by which each user is identified to a computer system.
- 7.28 West Virginia Division of Personnel – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.
- 7.29 West Virginia Office of Technology (OT) - The organization led by the State’s CTO and designated to acquire, operate, and maintain the State’s technology infrastructure. The OT is responsible for evaluating equipment and services, and reviewing information technology contracts.
-

8.0 LEGAL AUTHORITY

The CTO is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO has authority to issue policies, procedures, and standards to accomplish this mission. This policy will apply across the Executive Branch, with the exclusion of the West Virginia State Police, the Division of Homeland Security and Emergency Management, any constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than Information Security policies issued by the West Virginia OT, the more restrictive provisions will prevail.

This policy is consistent with the following federal and state authorities:

- W. Va. Code § 5A-6-4a

Policy: Information Security

State of West Virginia Office of Technology

- NIST SP 800-14 and NIST SP 800-53
- Omnibus Reconciliation Act of 1990, § 2201(c), 42 U.S.C. § 405(c)(2)(C)(viii)(I).
- Health Insurance Portability and Accountability Privacy Rule, 45 CFR 160 and 164
- Confidentiality of Substance Abuse Records, 42 U.S.C. 290dd-2; 42 CFR Part 2
- Gramm-Leach Bliley Act (GLBA), 15 U.S.C. § 6801, 16 CFR § 313
- Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*
- Driver’s Privacy Protection Act, 18 U.S.C. § 2721
- Telemarketing Sales Rules, 16 CFR Part 310
- Executive Order No. 7-03 (March 25, 2003)
- Freedom of Information Act, W. Va. Code § 29B-1-1 *et seq.*
- Records Management and Preservation of Essential Records Act, W. Va. Code §§ 5A-8-21, 22
- State Health Privacy Laws, www.wvdhhr.org/hipaa/privacy.asp
- Confidentiality and Disclosure of Tax Returns and Return Information, W. Va. Code § 11-10-5d
- Uniform Motor Vehicle Records Disclosure Act, W. Va. Code 17A-2A-1 to1

9.0 INDEX

A

Acceptable Use	1, 6, 9, 15, 19
Access.....	8
Access Controls	3, 8
Administrative Responsibilities.....	2
Agency Head	2, 6, 9
Appendix A	15
Authentication	4, 8

B

Background.....	1
-----------------	---

C

Cellular Phones and other Wireless Devices	17
Chief Information Security Officer.....	See CISO
Chief Technology Officer.....	See CTO
CISO	7, 8

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001 Issue Date: 01/18/07 Revision Date: Page 13 of 20

Classification of Information	5
Confidential/Sensitive Data	4, 9, 17
Confidentiality Agreement	6
Contractor	9
Critical Data.....	8
CTO.....	1, 2, 3, 4, 7, 8, 9, 11
Custodian of Information.....	See Information Custodian

D

Definitions	8
Disciplinary Action.....	See Enforcement

E

E-Mail.....	6, 7, 16, 17
Employee Background Check	6
Employee Responsibilities.....	4, 6, 8, 16, 17, 18, 19
Employees	1, 5, 6, 7, 9, 10, 16, 17, 18, 19
Encrypted Data	4
Enforcement	8
Equipment Protection	8
Executive Branch	1, 8, 10, 11, 12

G

Governor's Executive Order No. 6-06	1
---	---

I

Incident Management Teams.....	3
Information Access	3, 5, 15
Information Assets.....	4, 9
Information Custodian	5
Information Disclosure	5, 12
Information Disposal/Destruction.....	5
Information Distribution.....	5
Information Owner	4, 5, 19
Information Resource Facilities.....	7
Information Resources	1, 2, 3, 5, 6, 9, 10
Information Security.....	1, 3, 7, 9, 10, 11, 15, 18
Information Security Administrator.....	See ISA
Information Security Liaisons	See ISL
Information Technology	1, 9, 10
Internet Monitoring and Filtering	6
ISA.....	2, 3, 5, 9, 10
ISL	2, 10
IT Assets.....	2
IT Resources	1, 5, 6, 16, 19

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001 Issue Date: 01/18/07 Revision Date: Page 14 of 20

L

Legal Authority11

M

Medium3, 10

N

Network4, 8, 9, 10, 16, 17

O

OT1, 2, 3, 6, 8, 9, 11, 16, 17

OT Service Desk6, 7

Owner of Information See Information Owner

P

Password4, 10, 17, 19

Personal Use5, 16, 17, 18

Personally Identifiable Information4, 10

Personnel Practices5

Physical and Environmental Security7

Policy and Procedure Training6, 9

Privacy Officer7, 10

Procedures3, 10

Purpose1

R

Relevant Documents/Material2

Relevant Technologies15

Responsibility/Requirements2

Risk Analysis3, 10

Risk Management3

S

Scope1

Security Breaches19

Security Contact10

Security Incident3, 10

Security Threats7, 10, 11

Security Violations7, 16, 17

Software2, 3, 9, 16, 19

T

Technology Usage Practices See Appendix A

Threat See Security Threat

Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001 Issue Date: 01/18/07 Revision Date: Page 15 of 20

U

Unacceptable Use.....	1, 6, 15, 18, 19
User	11
Userid	4, 11, 19
Users.....	2, 3, 7

V

Virus Control	6
---------------------	---

W

West Virginia Code 5A-6-4a	1
West Virginia Division of Personnel	6, 8, 11
West Virginia Office of Technology	See OT

Appendix A: Technology Usage Practices

State of West Virginia Office of Technology

Policy: **Information Security**

Acceptable/Unacceptable Use of State-provided Technology: Computers, E-mail, Internet Access, and Wireless Devices

The information contained within this Appendix applies to the State of West Virginia Information Security policy and the Acceptable Use of State-Provided Wireless Devices policy.

Relevant Technologies

Include, but may not be limited to the following:

- a. Personal computers
- b. Personal Digital Assistants (PDA)
- c. Fax or copy machines with memory or hard drives
- d. Internet or Intranet
- e. E-mail
- f. Voice Mail
- g. Cell phones (including camera phones and smart phones with data communications and databases)
- h. Pagers
- i. Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives)
- j. Servers
- k. Printers

Unacceptable uses include, but are not limited to the following:

- a. Any use which violates local, state, or federal laws;
- b. Any use for commercial purposes, product advertisements, or “for-profit” **personal** activity;
- c. Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
- d. Any use for promotion of political or religious positions or causes;
- e. Any use in relation to copyright infringement;

Appendix A: Technology Usage Practices

State of West Virginia Office of Technology

Policy: **Information Security**

- f. Any use in relation to downloading, attaching, changing, distributing, or installing any software or inappropriate files for non-business functions (ex: downloading MP3 files and/or broadcast audio or video files), including streaming content;
 - g. Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;
 - h. Any use for promoting harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability;
 - i. Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
 - j. Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
 - k. Any use for dispersing data to customers or clients without authorization;
 - l. Any use in relation to placing wagers or bets;
 - m. Any use that could be reasonably considered as disruptive to another's work;
 - n. Any sending or sharing of confidential information for unauthorized purposes;
 - o. Any personal use that can be construed as being other than minimal;
 - p. Any attachment or use of devices on the State network that are not owned by the State or authorized by the OT;
 - q. Redirecting State data to a non-State owned computing device or PDA on a routine basis, or without authorization from the CTO; or
 - r. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
1. Employees will not waste IT resources by intentionally doing one or more of the following:
 - a. Placing a program in an endless loop;
 - b. Printing unnecessary amounts of paper;
 - c. Disrupting the use or performance of State-provided IT resources or any other computer system or network; or
 - d. Storing unauthorized information or software on State-provided IT resources.
 2. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
 - a. Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;
 - b. Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
 - c. Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
 - d. Misrepresenting oneself or the State of West Virginia;

Appendix A: Technology Usage Practices

State of West Virginia Office of Technology

Policy: **Information Security**

- e. Making statements about warranty, express or implied, unless it is a part of normal job duties;
 - f. Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the OT; or
 - g. Transmitting through the Internet confidential data to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the OT.
3. Employees will not commit security violations related to e-mail activity. This includes doing one or more of the following:
- a. Sending unsolicited commercial e-mail messages, including the distribution of “junk mail” or other advertising material to individuals who did not specifically request such material;
 - b. Unauthorized use for forging of e-mail header information;
 - c. Solicitation of e-mail for any other e-mail address, other than that of the poster’s account, with the intent to harass or to collect replies;
 - d. Posting messages to large numbers of users (over 50) without authorization; or
 - e. Posting from an Agency e-mail address to newsgroups, blogs, or other locations without a disclaimer stating that the opinions expressed are strictly their own and not those of the State or the Agency, unless posting is in the fulfillment of business duties.
4. Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.

Cellular Phones and other Wireless Devices

State-provided wireless devices are made available to any employee, who by the nature of their work, must be accessible at any time of day, day of the week, or from any location. The State has the right to monitor and review these devices for operational or management purposes.

- 1. Wireless Services include, but are not limited to, voice, data, text messaging, voicemail, caller ID, call waiting, call forwarding, and three-way calling.
- 2. Wireless devices are intended to provide the means for staff to conduct State business in environments when landlines or computer networks are not available. Personal use of wireless devices and service is prohibited except in certain limited and occasional circumstances that meet with the supervisor’s approval. Personal use should only occur when it does not (1) interfere with the employee’s work performance; (2) interfere with the work performance of others; (3) have undue impact on business operations; or (4)

Appendix A: Technology Usage Practices

State of West Virginia Office of Technology

Policy: **Information Security**

violate any other provision of this policy or any other State policy, procedure, or standard. Use of wireless devices is a privilege that may be revoked at any time. The State reserves the right to address excessive personal usage and recover the cost of excessive personal usage from the user. The following list should assist in setting a standard for **limited non-business use**:

- a. To alert household members about working late or other schedule changes;
- b. To make alternative child care arrangements;
- c. To talk with doctors, hospital staff, or day care providers;
- d. To determine the safety of family or household members, particularly in an emergency;
- e. To make funeral arrangements;
- f. To reach businesses or other parties that can only be contacted during work hours; or
- g. To arrange emergency repairs to vehicles or residences.

Unacceptable uses of State-provided wireless devices include, but may not be limited to the following:

1. Using the wireless device to make 900-number and toll calls;
2. Purchasing and downloading games, ring tones, and/or non-business related subscription services;
3. Using the wireless device while driving, without the use of a hands-free device, such as a headset, ear bud, or installation kit;
4. Using the wireless device to make directory assistance calls (Exceptions include emergency or unavoidable use);
5. Using the wireless device to call State toll-free numbers (State incurs double costs); and
6. Excessive personal use or personal use that causes additional charges on the invoice.

Employees must ensure that all non-business calls that cause incremental charges to the invoice are made at the employee's own expense, (e.g., charged to personal calling or credit cards, home telephones, or other non-State subsidized telephone numbers), and do not increase air time charges to the State.

Employee Responsibilities

Employees should conduct themselves as representatives of the State, and are responsible for becoming familiar with and abiding by all Information Security policies and guidelines.

1. Employees will only access files, data, and protected records if:
 - a. The employee owns the information;
 - b. The employee is authorized to receive the information; or

Appendix A: Technology Usage Practices

State of West Virginia Office of Technology

Policy: **Information Security**

- c. The information is publicly available.
2. Employees are responsible for all activity that takes place through their user id. For example, employees must:
 - a. Always use strong passwords; and
 - b. NEVER share passwords with any individual for any reason.
3. Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following:
 - c. Logging off computer;
 - d. Locking computer; and/or
 - e. Locking file cabinets and drawers
4. Employees are prohibited from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.
5. Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.
6. Employees must report the following instances to a supervisor or designated security contact:
 - f. Receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
 - g. Becoming aware of breaches in security; or
 - h. Becoming aware of any inappropriate use of State-provided IT resource.
7. Employees must adhere to copyright law regarding the use of software, print or electronic information, and attributions of authorship. In certain instances, legal counsel can determine permissible uses.
8. Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.